APPARATUS AND METHOD FOR DISTRIBUTING LAYER-2 VPN INFORMATION

FIELD OF THE INVENTION

[0001] This invention relates to virtual private networks (VPNs) and, in particular, a method for outsourcing layer-2 VPN auto-discovery to a layer-1 and/or (G)MPLS-based VPN discovery mechanism.

BACKGROUND OF THE INVENTION

[0001] Many definitions of VPNs can be considered:

[0002] Definition 1: A VPN is a set of users (devices attached to the network) sharing common membership information and intended to establish inter-site connectivity (within that group). A user can be a member of multiple groups (VPNs).

[0003] Definition 2: A VPN is a client private network that subscribes to restricted connectivity services.

[0004] Definition 3: A VPN is a service where a customer requests multi-site connectivity services provided through a shared network infrastructure.

[0005] Definition 4: A VPN is a service where a partition of internal provider network resources is allocated to a customer.

[0006] Using specialized tunneling protocols and optionally secured encryption techniques, data integrity and privacy may be maintained in a VPN.

[0007] Categories of VPNs include layer-1, layer-2 and layer-3. "Layer-n" is in reference to the network layer used to perform the hand-off between the customer and provider network.

[0008] Layer-1 VPNs can be simple, point-to-point connections such as leased lines, ISDN links, or dial-up connections or Sonet/SDH/Optical private lines. They are known to be simple for the provider, as they place all responsibility for operating the network over the connection on the customer. In other words, the customer needs to provide and manage all the routing and switching equipment that operates over the connection.

[0009] Layer-2 VPN is a VPN in which the service provider connects customer sites using leased circuits connecting into a point of presence (POP) or node on a shared core network. Layer-2 VPNs are typically based on Frame Relay , ATM, or Ethernet. Exemplary VPN mechanisms at layer-2 include virtual private LAN service (VPLS) (see Waldemar Augustyn et al, "Requirements for Virtual Private LAN Services (VPLS)", October 2002) and virtual private wire (VPW) (see Eric Rosen et al, "L-2 VPN Framework", February 2003).

[0010] Layer-3 VPN is a VPN in which the service provider either supplies a leased IP-based circuit connection between the customer site and the nearest POP on the edge of the service provider network or the client outsource its layer-3 network to the service provider with respect to private route distribution. The service provider takes care of the routing and addressing of the customer traffic. The service provider distributes the IP addressing information for a company across all of its relevant sites. Exemplary VPN mechanisms at layer-3 include virtual routing (VR) – base mechanisms, such as VR using border gateway protocol (BGP) (see Hamid Ould-Brahim et al "Network-based IPN VPN Architecture using Virtual Routers", July 2002) or VPN-based RFC 2547 bis (see Eric Rosen, et al, "BGP/MPLS VPNs", October 2002).

[0011] There are various possible arrangements for unifying different types of VPNs. In one known network arrangement, two carriers are provided. The first carrier is a provider providing layer-2, or layer-2 and layer-3 VPN services. The second carrier is a sub-provider providing layer-1 or Generalized VPN (GVPN) services. GVPN service (which in this case the first carrier subscribes to) is a VPN

service that uses BGP as a VPN auto-discovery (VPN discovery is a process in which VPN routing information is distributed) and generalized multi-protocol label switching (GMPLS) (which will be discussed) as signaling and routing mechanisms. GVPN services can be layer-1 and/or layer-2/3 VPNs.

[0012] The known methods for running this network arrangement have problems. In at least one known method, a layer-2 provider edge device must implement a level-2 VPN auto-discovery mechanism. Here the operator needs to configure and manage n^2 or a large number of BGP with TCP sessions running on layer-2 VPN provider edge devices across layer-1 VPN connections.

SUMMARY OF THE INVENTION

[0013] An object of the present invention is to provide an improved apparatus and method for distributing layer-2 VPN information.

[0014] A further object of the present invention is to provide a network which simplifies the mode of operations on the layer-2 VPN provider edge-based device by eliminating the need for the layer-2 VPN provider edge-based device to implement a full VPN auto-discovery for layer-2 VPN services. Yet a further object is to provide a network which takes advantage of layer-1 VPN auto-discovery implemented on the carrier network by piggybacking layer-2 information on top of it. Also, the network provides layer-1 VPN providers with the ability to offer added-value services that extend to layer-2 VPN without requiring the layer-1 VPN provider to support and offer a complete suite/solutions of layer-2 VPN connection and services.

[0015] The present invention provides a network having the above features and additional advantages which will be evident in the reading of the description and drawings which follow.

[0016] According to a first aspect of the present invention, there is disclosed a network that includes a first carrier network. The first carrier network is employed by a layer-1 VPN service provider. Layer-1 VPN information is created within the first

carrier network. The network also includes a second carrier network. The second carrier network is employed by a different service provider. Layer-2 VPN information is created within the second carrier network. A BGP session is used in transmitting layer-2 VPN information from the second carrier network to the first carrier network. Note that this session can as well be used for normal BGP related features that include L1VPN discovery mechanism.

[0017] In one embodiment, an auto-discovery mechanism for the second carrier network is outsourced to the first carrier network.

[0018] According to another aspect of the invention, there is disclosed a method for distributing layer-2 VPN information including the steps of:

[0019] (1) using BGP sessions and a discovery mechanism of a layer-1 provider edge device to distribute received layer-2 VPN information to a remote layer-1 provider edge device;

[0020] (2) passing the layer-2 VPN information from the remote layer-1 provider edge device to an attached layer-2 provider edge device; and

[0021] (3) using the layer-2 VPN information to simplify operations for a layer-2 service provider.

[0022] In another embodiment, the method further includes the step of advertising layer-2 VPN discovery to the layer-1 provider edge device before the step of using the BGP sessions and the discovery mechanism, and at least one inter-carrier BGP session is a mechanism for the advertising.

[0023] According to yet another aspect of the invention, there is disclosed a network including a backbone and at least two provider edge devices. The at least two provider edge devices are connected to and work with the backbone. Layer-1 and layer-2 VPN information is processed by one of the at least two provider edge

devices. This provider edge device has a discovery mechanism for distributing the layer-2 VPN information.

[0024] In an alternative embodiment, the at least two provider edge devices are a part of a network of a first service provider, and both layer-1 and layer-2 VPN auto-discovery are carried out within the network of the first service provider.

[0025] Further features and advantages will become apparent from the following detailed description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0026] **FIG. 1** is a schematic diagram illustrating a network reference model within which the apparatus and method of the invention can be utilized according to an embodiment of the invention.

[0027] **FIG. 2** is a flow diagram illustrating a method of operation implementable in the model of **FIG. 1**, the method of operating being in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

[0028] Referring to **FIG. 1**, there is illustrated a network **10** connecting together VPNs **14** with remote VPNs **18**. The VPNs **14** are customer networks which interface with a provider network via customer edge routers **20**. Provider edge routers or switches **24** are associated with the provider network. The router **24** is a portion of the provider's network that interfaces with a particular VPN **14**. This provider or first carrier provides layer-2, or layer-2 and layer-3 VPN services to its customers.

[0029] The provider routers **24** also interface with a network **28** of a sub-provider or second carrier. The sub-provider's network **28** connects to the provider's network via a provider edge device **30**. The device **30** is a portion of the network **28**.

Portions of the network **28** may also interface with a backbone. An example of a backbone would be an Internet backbone. Of course those skilled in the art will appreciate that other types of backbones are possible.

[0030] The second carrier network includes one or more layer-1 VPN service bases. The second carrier provides layer-1 services or GVPN services to the first carrier.

[0031] GVPN service is a provider-provisioned VPN service that uses BGP as a VPN auto-discovery mechanism. BGP is an important protocol for VPNs and the Internet. BGP is also an Internet standard for inter-domain autonomous system (AS) exterior routing. Furthermore, BGP is the routing protocol employed on the Internet. All Internet Service Providers must use BGP to establish routing between one another.

[0032] GVPN service also uses GMPLS as a signaling and routing mechanism. One way of defining GMPLS is as follows. In a multi-protocol label switching (MPLS) network, incoming packets are assigned a label by a label edge router. Packets are forwarded along a label switch path where each label switch router makes forwarding decisions based solely on the contents of the label. At each hop, the label switch router strips off the existing label and applies a new label which tells the next hop how to forward the packet. GMPLS extends MPLS from supporting packet (PSC) interfaces and switching to include support of the following three classes of interfaces and switching: time-division multiplex (TDM), lambda switch (LSC) and fiber-switch (FSC).

[0033] The remote side of the network **10** can have an arrangement substantially mirroring the proximate side. A provider edge device **34** interfaces the network **28** with a remote network of a layer-2 VPN service provider. This remote service provider has a provider edge router or switch **36**. The router **36** interfaces the network of the layer-2 VPN service provider with the network **28**.

[0034] The router **36** also interfaces the remote network of the layer-2 service provider with one or more of the remote VPNs **18**. The VPNs 18 interface with the remote network of the layer-2 VPN service provider via customer edge routers **40**.

[0035] With respect to the layer-2 VPN provider edge routers or switches used in the network **10**, previous implementations required the layer-2 VPN provider edge router or switch to implement a layer-2 VPN auto-discovery mechanism. Also, the operator needed to configure and manage n square, or at least a large number of BGP and with TCP sessions running on layer-2 VPN connections.

[0036] In one embodiment of the apparatus and method for distributing layer-2 VPN information, layer-2 VPN information is communicated between a layer-2 VPN provider edge router or switch and the sub-provider during a BGP session. At the layer-1 provider edge device, BGP/TCP sessions are established for the purpose of distributing layer-1 and layer-2 VPN information. In previous solutions, these layer-1 provider edge device BGP/TCP sessions were established for the purpose of distributing layer-1 VPN information only. That meant that it was at the layer-2 provider edge device that BGP/TCP sessions were established for the purpose of distributing layer-2 VPN information.

[0037] **FIG. 2** is a flow diagram illustrating the method of operation for outsourcing layer-2 VPN auto-discovery to a layer-1 and/or GMPLS-based VPN discovery mechanism. Starting at step **60**, the BGP sessions are configured. For each layer-1 VPN service basis, one BGP session is set up between a layer-1 provider edge device (such as the device **30** of **FIG. 1**) and a layer-2 provider edge device (such as the device **24** of **FIG. 1**).

[0038] At step **62**, the layer-2 provider edge device uses the BGP sessions of step **60** to advertise layer-2 VPN discovery to the attached layer-1 provider edge device.

[0039] At step **64**, BGP sessions are established at the layer-1 provider edge device.

[0040] At step **66**, the BGP sessions of step **64** are used in combination with a layer-1 VPN discovery mechanism to distribute the layer-2 VPN information to all remote layer-1 provider edge device(s) (such as the device **34** of **FIG. 1**).

[0041] At step **68**, the remote layer-1 provider edge device(s) receive and pass the layer-2 VPN information to the attached layer-2 provider edge devices (such as the routers **40**).

[0042] Finally, at step **70**, the layer-2 VPN information is used within the first carrier network.

[0043] **Glossary of Acronyms Used**

BGP – Border Gateway Protocol
GMPLS – generalized MPLS
GVPN – generalized VPN
MPLS – multi-protocol label switching
VPLS – Virtual Private LAN Service
VPN – Virtual Private Network

[0044] While the invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications, and variations will be apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended to embrace all such alternatives, modifications, and variations as fall within the spirit and broad scope of the appended claims.